AO 106 (Rev. 04/10) Application for a Search Warrant AUSA Glenn-Applegate

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A certain cellular phone seized during the arrest of Charles Asumadu on February 1, 2022

Case No. 2:22-mj-126

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1956	Money Laundering
18 USC 1957	Money Laundering
18 USC 1343	Wire Fraud

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Shawn A. Mincks

Applicant's signature

Shawn Mincks, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence. VIA FACETIME

Date: 2/23/2022

Judge's signature

City and state: Columbus, OH

Elizabeth A. Preston Deavers, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

AFFIDAVIT
IN SUPPORT OF SEARCH WARRANT

I, Shawn Mincks, Special Agent, U.S. Department of the Treasury, Internal Revenue Service, Criminal Investigation, being duly sworn, depose and say that:

Introduction and Purpose

1. I am a Special Agent with IRS-Criminal Investigation and have been so employed since 2008. I have received specialized law enforcement training at the Federal Law Enforcement Training Center, Glynco, Georgia and additional specialized training from the IRS. My duties as a Special Agent include conducting investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code. I have participated in multiple such investigations, including several investigations related to individuals who launder funds derived from romance and other international fraud schemes.

2. I am assigned to pursue a federal criminal investigation of Charles Asumadu and other co-conspirators. I contend there is probable cause to believe that Asumadu and others were engaged in a conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h), and Asumadu personally committed or caused to be committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957. I further contend that evidence of such violations and evidence of wire fraud in violation of 18 U.S.C. § 1343, described in Attachment B, is located on or in the item described in paragraph #3 and Attachment A.

3. I make this affidavit in support of an application for a search warrant for a cellular phone seized by IRS-Criminal Investigation during the arrest of Asumadu on February 1, 2022. The item is further described as the following and is also described in Attachment A.

   Attachment A

   a. Rose Gold iPhone seized during the execution of an arrest warrant on Charles Asumadu

4. The device is currently in the possession of IRS-CI located at 401 North Front Street, Suite 375, Columbus, Ohio.

5. The information in this affidavit is either personally known to me based upon my experience, investigative activities, analysis of records and interviews; or it has been relayed to me by other agents and/or law enforcement personnel. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included

each and every fact know to me concerning the investigation. I have set forth only the facts I believe are necessary to support the requested search warrant.

Evidence of Probable Cause

Overview

6. Through interviews and analysis of bank records and other documentation, your affiant believes the investigation to date tends to show that Asumadu and others have been engaged in a conspiracy to commit money laundering in that they have knowingly and willfully facilitated the receipt, concealment and transfer of funds derived from so-called "Romance Scam" victims.

7. Perpetrators of the scams post fake profiles on various dating websites and social media applications, then individuals throughout the United States and other countries are contacted by or enticed to initiate contact with the perpetrators. After contacting the victims online, the perpetrators use email, instant messaging services, text messaging and phone calls to build a relationship of trust with the victims. Once trust is gained, the perpetrators convince the victims to provide money purportedly for various investments or need-based reasons. The perpetrators tell many of the victims that they are overseas. The perpetrators further explain, for example, that they have located a gold or diamond mine through which they can both become very wealthy if the victim invests money; or have had financial or legal trouble and need assistance. The perpetrators then contact bank account holders in the United States directly or through other intermediaries. The bank account holders include individuals such as Asumadu who are willing to accept fraudulent proceeds into their bank accounts. The victims then are directed by the perpetrators to wire transfer, direct transfer or deposit money into the bank accounts controlled by Asumadu and/or other co-conspirators. Evidence indicates that many of these bank accounts were opened in the names of business entities controlled by the co-conspirators. The victims provide the funds with the expectation that the money will be invested or used to assist their online "friend."

8. The funds are not used in the manner the victims believe it will be used. Contemporaneous and subsequent to the wire transfers, account transfers and deposits received by the Asumadu and the others from the victims, they disposed of the funds through cash withdrawals; checks and transfers to parties known to the co-conspirators; international and domestic wire transfers; personal expenditures; and purchases of official checks. None of the victims receive any return on their "investments" or any of their money back. The loss to all victims exceeds $5 million.

9. The affiant believes that evidence garnered so far in the investigation tends to show Asumadu and the others knew that the funds they were receiving and transmitting, or causing to be received and transmitted, were derived from some kind of unlawful activity, and the funds were, in fact, derived from a specified unlawful activity, namely wire fraud (18 U.S.C. § 1343). From the recipient bank accounts, the funds were not used in the manner promised to the victims of the fraud. Instead, the funds were

transacted in a fashion designed to conceal the nature, source, location, ownership and control of the funds through cash withdrawals and other mechanisms, in violation of 18 U.S.C. § 1956 (a)(1)(B)(i). Additionally, many debits were in excess of $10,000, in violation of 18 U.S.C. § 1957. Since they were working in concert with each other, as well as the perpetrators of the Romance Scams, the activity was in violation of 18 U.S.C. § 1956(h).

10. On January 28, 2022, the affiant filed a Criminal Complaint accusing Asumadu of violations of 18 U.S.C. §§ 1956(h); 1956(a)(1)(B)(i); and 1957. As a result of the filing of the Criminal Complaint, an arrest warrant was issued for Asumadu.

11. On February 1, 2022, the affiant and other IRS-CI Special Agents executed the arrest warrant and apprehended Asumadu outside his residence located at 3364 Thornapple Circle North, Columbus, Ohio. After placing Asumadu into custody, the affiant asked Asumadu if he would like to go back inside his residence to discuss the arrest and charges. Asumadu stated that he would like to do so. The agents conducted a security sweep of the lower level of the residence and encountered Asumadu's wife. The agents explained to her the situation then allowed Asumadu to sit on the couch located on the lower level of the apartment. The affiant returned to his vehicle to retrieve a copy of the arrest warrant and some additional items leaving Asumadu with other Special Agents. After retrieving the documents, the affiant re-entered the apartment to rejoin the other agents and Asumadu. The affiant then read Asumadu his In-Custody Statement of Rights. Upon completion of the reading, the affiant asked Asumadu if he understood his rights. Asumadu stated that he understood the rights as read to him. The affiant then explained to Asumadu that they would be traveling to the IRS-CI office to continue the conversation. Before they exited the residence, the affiant asked Asumadu about the location of his phone. Law enforcement did not claim to have a warrant to seize the phone or otherwise claim that Asumadu had a legal obligation to provide his phone. Asumadu explained that he possessed a work phone, but it was at his work location. Asumadu then said he had a personal phone and spoke to his wife in a language other than English. Asumadu's wife retrieved the personal phone and gave it to Special Agent Kyle Borton. Special Agent Borton then gave the phone to the affiant. The phone was the Rose Gold iPhone for which this affidavit requests issuance of a search warrant.

Relevant Bank Accounts and Entities

12. Asumadu established Dr. C. Asumadu Health Care Agency on March 15, 2017 by filing documents with the Ohio Secretary of State located in Columbus, Ohio. Querying "Charles Asumadu" on www.docinfo.org, which is a nationwide database of licensed doctors, returns "No Results Found." Asumadu opened and controlled the business bank accounts below, among others, in the name of Dr. C. Asumadu Health Care Agency. Asumadu was the only signer on all accounts.

    a. March 16, 2017 – August 20, 2018: PNC Bank account # xx2138 (PNC xx2138).

b. June 19, 2017 – October 31, 2018: JP Morgan Chase Bank account # xx6262 (JPMC xx6262).

13. Asumadu also opened and controlled personal bank accounts on which he was the only signer. Some notable accounts are listed below.

a. November 30, 2015 – May 9, 2017: Fifth Third Bank account # xx1992 (FTB xx1992)

b. July 6, 2016 – December 8, 2016: US Bank account # xx6952 (US Bank xx6952).

c. October 31, 2016 – July 20, 2017: Bank of America account # xx6382 (BOA xx6382).

Witness Statements and Transactions

14. Law enforcement has interviewed or reviewed statements by several individuals who deposited, wired, or otherwise sent funds to bank accounts in the control of Asumadu. Consideration of the witness statements and analysis of bank accounts in Asumadu's control shows that between August 4, 2016, and May 8, 2020, Asumadu received more than $700,000 in funds from victims of romance fraud. He then conducted or caused to be conducted financial transactions to launder the fraud proceeds.

15. Review of the records of the bank accounts in Asumadu's control did not result in finding revenue or expenses that would be typical of a medical or health care company, such as payments from private insurance companies; payments from Medicare, Medicaid, or other government programs; purchases of medical supplies; and regular payroll to other individuals.

16. According to an interview with Person 3, whose identity is known to the affiant, Person 3 met somebody she believed to be named David Brown on social media in 2016 after her husband died. Person 3 communicated with Brown via social media and text messaging applications, and Brown eventually told Person 3 that he loved her. Brown asked Person 3 to send him money to start a business, and Person 3 expected to be repaid. After seeing a television special, Person 3 realized she was the victim of a scam. Bank records show that on September 6, 2016, Person 3 wired $15,000 to a PNC Bank account controlled by Conspirator 2. Bank records show that, after receiving the funds, Conspirator 2 engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds.

17. Bank records show that on December 15, 2016, Person 3 also deposited $3,000 cash into BOA xx6382, controlled by Asumadu.

18. Bank records show that after receiving the funds from Person 3 into BOA xx6382, Asumadu engaged in the following financial transaction involving the proceeds of wire

fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. December 16, 2016 - $2,900 transfer to FTB xx1992, controlled by Asumadu.

19. According to an interview with Person 4, whose identity is known to the affiant, Person 4 met somebody she believed to be named Michael Wayne James on social media approximately six years ago. Person 4 later also communicated with James via text. James told Person 4 he was in the military. Eventually, James asked Person 4 for money to assist him getting home. Person 4 later told James that she could not send any more money, and James "got nasty" with her. Person 4 then cut off communications with James. Bank records show that on October 17, 2016, Person 4 wired $12,700 to US Bank xx6952, controlled by Asumadu.

20. Bank records show that after receiving the funds from Person 4 into US Bank xx6952, Asumadu made withdrawals of an unknown nature of $5,000 and $5,014 on October 18, 2016.

21. According to an interview with Person 5, whose identity is known to the affiant, Person 5 met somebody she believed to be named Giovani Bellini on a dating website sometime in 2017. Person 5 and Bellini communicated several times a day, every day, via texts and calls. Bellini told Person 5 that he lived in Georgia but had gotten a construction contract in Ghana. After arriving in Ghana, Bellini began to ask Person 5 for money supposedly for expenses related to the contract. After approximately six months of sending money, Bellini told Person 5 she should get a loan on her home. Person 5 realized that she was being scammed. Bank records show that between March 20, 2017 and April 4, 2017, Person 5 deposited $24,000 cash into BOA xx6382, controlled by Asumadu.

22. Bank records show that on March 6, 2017 and March 22, 2017, Person 4 also deposited $6,000 cash and $22,800 in the form of personal check, respectively, into BOA xx6382, controlled by Asumadu.

23. Bank records show that on April 3, 2017, Person 3, also deposited $2,000 cash into BOA xx6382.

24. Bank records show that after receiving the funds from Person 3, Person 4 and Person 5 into BOA xx6382, Asumadu engaged in the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. March 6, 2017 - $5,300 transfer to FTB xx1992, controlled by Asumadu;

b. March 16, 2017 - $6,900 wire to PNC xx2138, controlled by Asumadu;

c. March 27, 2017 - $4,700 wire to PNC xx2138, controlled by Asumadu;

d. March 27, 2017 - $4,400 transfer to PNC xx2138, controlled by Asumadu;

e. March 29, 2017 - $16,036 wire to Company 1 in Ghana;

f. March 30, 2017 - $1,500 transfer to PNC xx2138, controlled by Asumadu;

g. April 4, 2017 - $14,165 wire to Company 1 in Ghana.

25. Bank records show that on April 13, 2017, Person 5 also deposited $12,000 cash into a Bank of America account controlled by Conspirator 2.

26. Bank records show that after receiving the funds from Person 5 into the Bank of America account, Conspirator 2 engaged in the following financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. April 13, 2017 - $11,000 wire to Company 1 in Ghana.

27. According to an interview with Person 8, whose identity is known to the affiant, Person 8 met somebody she believed to be named James Logan a few years ago on social media during a time when her marriage was falling apart. Logan claimed he was a military doctor serving in Afghanistan. Logan later convinced Person 8 to send money to pay fees related to an alleged inheritance consisting of cash, gold and jewelry. Person 8 eventually realized she had fallen victim to a scam and filed a complaint with the FBI. Bank records show that on June 21, 2017, a cashier's check in the amount of $15,000 purchased by Person 8 was deposited into a Bank of America account, controlled by Conspirator 2.

28. Bank records show that the funds from Person 8 were commingled with other funds in the Bank of America account. Conspirator 2 then engaged in the following financial transaction, among others, involving the proceeds of wire fraud with the commingled funds. The transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. June 29, 2017 - $22,000 wire to Company 1 in Ghana.

29. Bank records show that on June 26, 2017, Person 8 also wired $10,000 to JPMC xx6262, controlled by Asumadu.

30. Bank records show that after receiving the funds from Person 8 into JPMC xx6262, Asumadu engaged in the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. June 27, 2017 - $5,500 cash withdrawal;

b. June 27, 2017 - $3,000 ATM cash withdrawal.

31. According to an interview with Person 9, whose identity is known to the affiant, Person 9 met somebody she believed to be named David Schwartz on a dating website sometime in 2016 or 2017. Schwartz communicated with Person 9 via email and a phone application. Schwartz told Person 9 he was in Turkey on an oil platform. Schwartz eventually asked Person 9 to send him money for his goddaughter who had been arrested and after his mother allegedly died. Person 9 sent money at Schwartz's direction and expected to be repaid. She was not repaid. Bank records show that on August 10, 2017, Person 8 wired $12,000 into PNC xx2138, controlled by Asumadu.

32. Bank records show that the funds from Person 9 were commingled with other funds in PNC xx2138. Asumadu engaged in the following financial transaction, among others, involving the proceeds of wire fraud with the commingled funds. The transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. August 11, 2017 - $10,955 wire to Company 1 in Ghana.

33. Bank records show that on December 11, 2017, a cashier's check in the amount of $40,000 purchased by Person 9 was deposited into a JP Morgan Chase Bank account controlled by Conspirator 2.

34. Bank records show that after receiving the funds from Person 9 into the JP Morgan Chase Bank account, Conspirator 2 engaged in the following financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. December 13, 2017 - $23,003.15 wire to Company 1 in Ghana;

b. December 19, 2017 - $13,600 wire to Company 1 in Ghana.

35. According to an interview with Person 10, whose identity is known to the affiant, Person 10 met somebody she believed to be named Kevin Alberto on a dating app. Alberto told Person 10 he was on a ship and needed money to get off the ship and into the United States. Alberto instructed Person 10 to send money to his friends, Conspirator 3 and Conspirator 4. Person 10's bank eventually advised her that she was likely involved in a fraudulent scheme. Bank records show that on September 25, 2017, Person 10 wired $22,500 to PNC xx2138, controlled by Asumadu.

36. Bank records show that the funds from Person 10 were commingled with other funds in PNC xx2138. Asumadu engaged in the following financial transactions, among others, involving the proceeds of wire fraud with the commingled funds. The transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. September 25, 2017 - $8,000 cash withdrawal;

b. September 26, 2017 - $9,500 cash withdrawal.

37. According to an interview with Person 13, whose identity is known to the affiant, Person 13 was contacted on social media several years ago by somebody she believed to be named James Stewart. Stewart told Person 13 that he was from San Diego but was serving in the army in Syria. Eventually, Stewart told Person 13 that his father had sold a business and acquired some assets. Stewart asked Person 13 for money to secure the assets and pay for his travel home. Person 13 sent money to pay for alleged fees at Stewart's request before her son and daughter discovered she was being scammed. Bank records show that on April 6, 2018, Person 13 purchased a cashier's check in the amount of $50,000 payable to Dr. C. Asumadu Health Care Agency. The check was deposited into JPMC xx6262, controlled by Asumadu, the same day.

38. Bank records show that after receiving the funds from Person 13 into JPMC xx6262, Asumadu engaged in the following financial transactions, among others, involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. April 7, 2018 - $30,000 transfer to an account controlled by a third party;

b. April 7, 2018 - $5,000 cash withdrawal;

c. April 7, 2018 - $3,000 ATM cash withdrawal;

d. April 11, 2018 - $3,000 ATM cash withdrawal;

e. April 11, 2018 - $2,000 cash withdrawal.

39. Bank records show that on June 19, 2018 Person 13 transferred $5,000 from her JP Morgan Chase Bank account into a JP Morgan Chase Bank account controlled by Conspirator 2.

40. Bank records show that the funds transferred to the JP Morgan Chase Bank account were commingled with other funds. Conspirator 2 engaged in the following financial transaction, among others, involving the proceeds of wire fraud with the commingled funds. The transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

a. June 20, 2018 - $19,700 wire to Company 1 in Ghana.

41. Bank records show that on June 20, 2018 Person 13 transferred $6,000 from her JP Morgan Chase Bank account into a JP Morgan Chase Bank account controlled by Conspirator 2.

42. Bank records show that the funds transferred to the JP Morgan Chase Bank account were commingled with other funds. Conspirator 2 engaged in the following financial transaction, among others, involving the proceeds of wire fraud with the commingled funds. The transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    a. June 22, 2018 - $4,000 check issued to Conspirator 4.

43. Person 13 provided documentation to the affiant on which she stated that, in addition to those funds sent to Asumadu and Conspirator 2, she sent funds to Conspirator 3 at Stewart's direction.

44. According to a complaint filed on the FBI Internet Crime Complaint Center (IC3) on November 30, 2017 by Person 15, whose identity is known to the affiant, Person 15 met somebody she believed to be named Christopher Brooks on a dating website. Brooks told Person 15 he was in the oil businesses and his partner was injured in a hurricane. Brooks convinced Person 15 to send money to different recipients related to the alleged injury and oil business, including to Conspirator 4 and Conspirator 5.

    a. According to her complaint, Person 15 provided $40,000 to Conspirator 5 between September 22, 2017 and September 26, 2017. On September 29, 2017, Conspirator 5 purchased a cashier's check payable to Dr. C. Asumadu Health Care. The check was deposited on the same day into JPMC xx6262, controlled by Asumadu.

45. According to a complaint filed on IC3 on April 12, 2018 by Person 16, whose identity is known to the affiant, Person 16 met somebody she believed to be named John Brown on social media. Brown told Person 16 he was in the army in Syria. Brown eventually began asking Person 16 for money to assist him getting home. Person 16 sent money Dr. C. Asumadu Health Care Agency at Brown's request. Bank records show that between February 26, 2018 and April 2, 2018, Person 16 wired $11,150 to JPMC xx6262, controlled by Asumadu.

46. According to a complaint filed on IC3 on April 29, 2020 by Person 18, whose identity is known to the affiant, Person 18 agreed to accept a package on behalf of somebody she believed to be named Charles Cowherd. As part of the agreement, Cowherd asked Person 18 to pay fees related to the package. Person 18 made payments to Copnspirator 2, Conspirator 4 and others. Bank records show that on April 13, 2020, Person 18 wired $10,000 to a TD Bank account controlled by Conspirator 2.

Use of Electronic Devices Generally and Apple Devices Specifically

47. I contend that Asumadu and others involved in the scheme described herein use various electronic devices to communicate with each other and other co-conspirators regarding and in facilitation of the fraud schemes and money laundering activities. This contention

is based upon extensive investigative experience into these schemes; witness statements; statements made by Conspirator 3; and my examination of records from Apple.

48. I know from investigative experience that individuals involved in these types of schemes will often take "screenshots" and photos as proof of their banking activities so that they can transmit the images to other co-conspirators. Furthermore, these images are often saved on iPhones and backed up into iCloud accounts. When new iPhones are purchased, the data from the iCloud account is often restored onto the new phone.

49. I also know from investigative experience that schemes such as these are facilitated by cell phone applications such as WhatsApp. WhatsApp is a smart phone application which can also be accessed via a computer. WhatsApp is a free instant messaging and voice over internet protocol service. The user of the application downloads the application to their phone and/or computer, and the application requires the user to assign a phone number to the application. After a phone number is assigned to the application, the application sends a verification text to the phone number assigned. In this way, the application is linked to the phone number of the phone onto which the application was downloaded. WhatsApp can then be used to transmit text messages, audio files, video files, image files and other electronic data.

50. I also know that smart phone applications such as WhatsApp are often installed on the phones of the perpetrators of fraud schemes such as this. This application is used by persons engaged in fraud to communicate with individuals while potentially disguising their true identities. These communications can include communications with co-conspirators as well as victims.

51. Information gathered to date implies that the locations of the various participants in the schemes and the rapid nature of the transactions necessitates use of cell phone applications to facilitate interstate and international communications between the victims, scammers, middlemen, and bank account holders.

Conspirator 3 and Conspirator 4

52. Between March 23, 2018 and February 4, 2020, Conspirator 2 issued checks and wires payable to Conspirator 3 and Conspirator 4 totaling at least $542,740 from bank accounts he controlled and into which funds from romance fraud victims were deposited. Also, as previously stated, Person 10 and Person 13 both sent funds to Conspirator 3.

53. Conspirator 3 and Conspirator 4 were arrested on November 16, 2020 after being charged with money laundering conspiracy in connection with romance fraud committed between May 2017 and October 2020. On October 29, 2021, Conspirator 3 and Conspirator 4 were sentenced to prison after pleading guilty.

54. Conspirator 3 was interviewed by Special Agents with FBI, Secret Service and the U.S. Postal Inspection Service on January 25, 2021. Conspirator 3 stated the following:

a. Conspirator 4 is his brother.

b. Conspirator 3 previously attended school in Ghana with Conspirator 2.

c. Conspirator 2 introduced Conspirator 3 to romance fraud and explained that Conspirator 3 could use his business bank account to send and receive money because the banks would be less suspicious of the transactions.

d. Conspirator 3 illustrated the different levels of the romance fraud scheme. The people that talk to the victims are at the top. These individuals are in Ghana and Nigeria. Conspirator 3 has never met these people. After the individuals in Ghana and Nigeria trick the victims into sending money, these individuals pass the information to middlemen. The middlemen reach out to individuals such as Conspirator 2 in the United States. Conspirator 2 recruits individuals willing to use their bank accounts to receive money from victims and then send the funds to the middlemen.

e. Conspirator 3 described the money arrangement with the other conspirators. He and Conspirator 2 evenly split ten to fifteen percent of the total fraud proceeds. The remaining fraud proceeds were sent to middlemen. Conspirator 3 has never met the middlemen, but he has spoken with one of them on the phone several times and has seen a picture of him on Snapchat.

f. Conspirator 3 described another method of moving the proceeds from the fraud scheme. On some occasions, he would make payments to online automobile auction websites that sold salvaged vehicles. The payments were made by Conspirator 3 on behalf of other people's "buyer accounts." The payments would be for the purchase of vehicles for individuals in Ghana. The individuals would then give money to the middleman in Ghana. Conspirator 3 received the vehicle information directly from the middleman via WhatsApp. Conspirator 3 stated the middleman with whom he communicated had two WhatsApp accounts.

g. Conspirator 3 and Conspirator 2 recruited another individual to accept money from the schemes. Conspirator 3 and Conspirator 2 lied to the recruit regarding the source of the funds. They told her the funds were not derived from illegal activity. Conspirator 3 communicated with the recruit in person, on the phone, through Snapchat, and other means.

55. Your affiant reviewed records provided by Apple. The records showed the following:

a. Apple ID asumadu.1@osu.edu is assigned to "Charles Asumadu" of 4362 Thornapple Circle West, Columbus, Ohio and 3364 Thornapple Cit (sic) North, Columbus, Ohio. The Apple records further show that the account was backed up hundreds of times to iCloud between March 2020 and April 2020.

Technical Background

56. Based upon my training and experience, I use the following technical terms to convey the following meanings:

a. Cell Phone/Mobile Device: A cell phone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

57. Based upon my training, experience and research, I know that the device for which the warrant is requested has capabilities to allow it to serve as a cell phone, digital camera, portable media player, GPS navigation device and PDA.

58. I have consulted with IRS-CI Special Agent-Computer Investigative Specialist Ebenger-Balla regarding the aspects of properly retrieving and analyzing electronically stored digital data. Special Agent Ebenger-Balla has been employed with IRS-CI since 2009. In addition to attending training in financial investigation techniques and accounting, she also completed the IRS-CI Basic Computer Evidence Recovery Training class at the Federal Law Enforcement Training Center in Glynco, Georgia, (2016) and the Advanced Computer Evidence Recovery Training class at the CyberCrimes Center in Fairfax, Virginia (2017), and Macintosh Forensics Training in Glynco, Georgia (2017). Special Agent Ebenger-Balla also completed the Mobile Device Forensics Training in Glynco, Georgia (2017) where she learned about the operation of mobile devices and the correct procedures for seizing and analyzing those devices.

59. Based upon the affiant's knowledge, training, experience and consultation with Special Agent Ebenger-Balla, the affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

60. As further described in Attachments B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium

61. The affiant knows that searching and seizing information from computers and cell phones often requires agents to seize most or all electronic storage devices to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

a. Technical requirements: Searching computer systems, such as cell phones, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

b. The volume and nature of electronic evidence: The volume of evidence. Computer storage devices such as cell phones can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

62. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

63. Based on the information presented in this affidavit, I contend that Asumadu and others were engaged in a conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h). I further contend that Asumadu and others committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957 in furtherance of the conspiracy. I further believe that Asumadu and others used various electronic devices, namely their cell phones, to communicate regarding and to facilitate the laundering of funds derived from fraud schemes, and evidence of these violations, as well as violations of 18 U.S.C. § 1343, is now located in the item described in Attachment A. Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Shawn A. Mincks
Special Agent, IRS-CI

Subscribed and sworn to before me

This 23rd day of February, 2022.

THE HONORABLE ELIZABETH A. PRESTON DEAVERS
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a "Rose Gold" iPhone cell phone seized during the arrest of Charles Asumadu on February 1, 2022.

Hereinafter, this cellular phone will be referred to as "the Device." The Device is currently located at 401 North Front Street, Suite 375, Columbus, Ohio.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that are evidence of violations of 18 U.S.C. § 1343 (wire fraud); any section of 18 U.S.C. § 1956 (money laundering) and/or 18 U.S.C. § 1957 (money laundering), for the period August 1, 2016, to the present, including:

   a. Records related to the wire-fraud scheme and money-laundering scheme described in the Affidavit;

   b. Records identifying the establishment, ownership, operation and/or control of any limited liability corporation or other business entity including articles of organization; correspondence with and/or submissions to/from any Secretary of State office; applications, disposition records and/or correspondence related to the issuance or use of Employer Identification Numbers (EIN); minutes and other official business records; and documents identifying any registered agent(s), incorporator(s), and/or other identified members;

   c. All records related to or referencing electronic transfers of funds or cash deposits including requests for an electronic transfer or cash deposit, wiring or deposit instructions, receipts, and correspondence;

   d. All records related or referring to persons or entities in other countries and the locations of such persons or entities;

   e. Asset ownership and/or acquisition records including contracts, invoices, receipts, registrations, titles insurance records and/or photographs of assets including motor vehicles, real property, boats, jewelry, precious metals and gems, and currency (foreign, domestic, or virtual currency);

   f. Travel records including travel directions, hotel reservations, rental car reservations, airplane reservations, invoices, airline tickets, and itineraries;

   g. Records related to banking activity including communications and data related to the opening, closing, use, custody and/or control of bank accounts, alternative currency accounts (i.e. those related to Bitcoins), credit cards, and/or debit cards including applications for accounts; approval or declination notices; credit and/or debit card issuance notices; credit and/or debit card activations; bank statements; welcome or account opening/closing notifications; deposit, payment, withdrawal, or transfer orders, receipts and/or notifications; balance inquiries and/or notices; and security notifications;

   h. All financial statements, accounting records and supporting source documents relating to receipts, expenditures, general ledgers, accounts and notes receivable, accounts and notes payable, balance sheets, income statements, statements of profit

and loss, and any other accounting records and other records and/or ledgers relating to Dr. C. Asumadu Healthcare, Dealership & Healthcare, LLC or any variation of these entity names or any other entities identified through items seized pursuant to section a. above;

i. Records pertaining to any financial institution account including but not limited to account numbers, passwords, personal identification numbers (PINS), deposit/withdrawal records, notes, logs, and photographs;

j. Electronic records of internet sites visited and data accessed and/or communications made in the course of visiting such internet sites;

k. Communications records and histories made through and/or from applications (known as "Apps"); emails; texts; calls or other media contained on the electronic devices to be searched and all attachments included in such communications; and

l. Contact lists and any documents reflecting names, addresses, email addresses, telephone numbers, fax numbers and/or other contact information.

m. Evidence indicating the cell phone owner's or user's state of mind as it relates to the crimes under investigation.

2. Evidence of user attribution showing who used or owned the cell phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.